THOMSON REUTERS
PRACTICAL LAW™

Drafting a Document Retention Policy

by Jonathan M. Redgrave, Amanda Moeller, and Daniel Zagoren, Redgrave LLP, with Practical Law Litigation

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **content.next.westlaw.com/0-506-7349**
Request a free trial and demonstration at: **tr.com/practicallaw-home**

A Practice Note explaining the key issues counsel should consider when drafting a document retention policy (DRP) (also referred to as a records and information management policy, a recordkeeping policy, or an information governance policy). This Note describes the objectives of a DRP, guidelines provided by leading authorities on information management, and practical steps to help ensure effective implementation of the DRP.

A document retention policy (DRP) provides the framework for a company's records and information management program. An effective DRP provides:

- Direction to company personnel on how they should manage information created or used in the course of the company's business operations.
- Guidelines to safeguard a company's records and proprietary information, which helps the company manage and reduce operational, reputational, and litigation risks.

When developing a DRP, counsel must consider the company's particular legal and business needs, including:

- The company's:
  - industry;
  - geographical location and locations of operation;
  - structure;
  - culture; and
  - technological environment.
- The types of information the company maintains.
- How information flows inside and outside the company.

In addition to evaluating the company's specific needs, when drafting a DRP, counsel should consider:

- The key objectives of the DRP (see Objectives of a DRP).
- Guidelines provided by leading authorities on information management (see Information Management Frameworks).
- Practical steps to help ensure effective implementation of the DRP (see Practical Considerations).

See Standard Document, Document Retention Policy for a sample DRP and Document Retention Policy: US Checklist for more on the considerations and steps involved in drafting a DRP.

Objectives of a DRP

The main objectives of a DRP are to:

- Explain the key terms and concepts related to managing company information (see Explain Key Terms and Concepts).
- Instruct employees about company information subject to retention requirements (see Identify Records and Information Subject to Retention Requirements).
- Outline the roles and responsibilities of employees for managing company information (see Define Employee DRP Roles and Responsibilities).

Explain Key Terms and Concepts

A DRP should explain and define concepts that are critical to understanding the DRP. Employees must appreciate that information is a vital company asset that must be appropriately managed throughout its lifecycle, which includes both retaining and disposing of information in accordance with the DRP.

In particular, the DRP should:

- State that company information is owned by the company.
- Explain what makes information a "record."
- Highlight the importance of records management.

- Address applications that should not be used to create records.
- Identify who is responsible for managing the records program.
- Clearly delineate employee records management responsibilities.
- Describe the consequences of non-compliance.

The DRP should define key terms using common, nontechnical language wherever possible, including the meaning and significance of:

- Records (see Records and Disposable Information).
- Disposable information (see Records and Disposable Information).
- Records retention schedules (see Records Retention Schedules).
- Legal holds (see Legal Holds).

When drafting definitions, counsel may find it useful to check with employees who are not information governance specialists to ensure that the definitions are clear and understandable.

Records and Disposable Information

For employees to appropriately manage company information, they must be able to distinguish types of records and information. For the purposes of this Practice Note, "records and information" includes :

- **Records.** Records reflect information that is created, transmitted, or received in the course of company business that the company must retain or wants to retain for business, regulatory, or legal purposes (see Identify Information Subject to Retention Requirements). A company will retain information for the period specified in the company's records retention schedule (see Records Retention Schedules) where the information:
  - serves as the company's corporate memory of an action, decision, or statement;
  - has enduring business value (for example, where the information provides a record of a business transaction, evidences the company's rights or obligations, protects the company's legal interests, or ensures operational continuity); or
  - is subject to legal, accounting, or other regulatory requirements.
- **Disposable information.** Disposable information, also often referred to as "non-records," consists of information that is not a record, and is redundant, obsolete, or trivial in nature, including, but not limited to:
  - Casual correspondence.
  - Drafts of documents that have been superseded by approved, official versions.
  - Personal documents and communications.
  - Unsolicited communications received from third parties.
  - Published literature, catalogs, and trade journals.
  - Duplicates or "convenience" copies of records that have not been annotated.

  A company typically should discard or delete disposable information once it no longer serves a useful business purpose and there is no other requirement to keep it. However, a company must preserve disposable information that is subject to a legal hold, even if the information no longer serves a useful purpose (see Legal Holds).

In addition to explaining the distinctions between records and disposable information, a DRP should reinforce the idea that these categories are media-neutral. It should clearly define records and disposable information to include information in paper or electronic format, as well as physical objects. For example, in the manufacturing context a sample widget may constitute a research and development or quality assurance record. Similarly, information in database fields may constitute records.

Further, the DRP should recognize and reflect that destruction is an important stage in the lifecycle of both records and disposable information. As the US Supreme Court stated in *Arthur Andersen LLP v. United States*, destruction of information under a valid DRP is not wrongful under ordinary circumstances (544 U.S. 696, 704 (2005)). Federal Rule of Civil Procedure (FRCP) 37(e) establishes the federal standard for evaluating a company's actions under a DRP and whether those actions may result in sanctions when information is lost that should have been preserved for legal matters. The Advisory Committee's Note states that the sanctions provision "does not apply when information is lost before a duty to preserve arises" (2015 Advisory Committee's Note to FRCP 37(e)).

See Sanctions in Federal Court Toolkit for a collection of resources to help counsel understand, avoid, and seek sanctions in federal civil litigation and arbitration.

Records Retention Schedules

Records retention schedules provide a straightforward way to instruct employees on how long they must keep company records. Typically, a records retention schedule is a series of charts that lists in separate columns:

- **The categories of records a company creates, receives, or uses in the ordinary course of business.** This information is usually organized by department, business process, or function. The records retention schedule should name or describe the record categories with sufficient detail to allow employees to identify which category applies to a specific record.
- **The length of time the company must retain each record category.** Retention time periods are often based on a combination of legal and business factors.

A basic retention schedule might use the following format:

RECORD	RETENTION PERIOD
Personnel Records	
I-9 Forms	The later of 3 years after hiring or 1 year after separation
W-2 and W-4 Forms	As long as the document is in effect +4 years
Corporate Records	
Articles of Incorporation, Bylaws, Corporate Seal, Minutes	Permanent

For a sample records retention schedule, see Standard Document, Document Retention Policy.

The amount of detail or specificity in a retention schedule will vary based on each company's business needs, legal obligations, regulatory obligations, and risk tolerance. Some records retention schedules include additional information, such as the departmental owner of the information, or provide additional requirements regarding the storage, management, or disposal of records. Companies may find that identifying the official repository for each category or type of records provides additional clarity and increases compliance (see Compliance). Similarly, companies may find that categorizing records into larger buckets makes schedules easier to administer and therefore facilitates compliance.

If applicable, a records retention schedule should include both the minimum and maximum time limits for retaining records. Maximum retention periods may be imposed by law, regulation, contract, or another external source and indicate the longest amount of time the company may retain the information. Some US laws specify maximum retention periods for specific types of records. For example:

- The Utah Employment Selection Procedures Act requires disposing of job applicant data within two years of when the applicant provides the information to the employer, unless the applicant is hired (Utah Code § 34-46-203(2)).
- The federal Video Privacy Protection Act requires the destruction of a customer's video rental records within one year from the date the information is no longer necessary for the purpose for which it was collected (18 U.S.C. § 2710(e)).

Until recently, it has been uncommon for US laws to specify maximum retention periods for specific record types. However, states are increasingly focused on maximum retention periods in the context of privacy laws. The California Consumer Privacy Act, which became effective January 1, 2020, provides that a business "shall not retain a consumer's personal information or sensitive personal information . . . for longer than is reasonably necessary" (Cal. Civ. Code § 1798.100(a)(3)).

Other states have passed laws mandating data minimization related to privacy and consumers' impacting the retention of personal information. (See, for example, 740 Ill. Comp. Stat. Ann. 14/15(a) (requiring businesses to establish a retention schedule for biometric identifiers and information and guidelines for the permanent destruction of such identifiers or information either after the business satisfies its initial purpose for collecting the identifiers or information, or within three years of the last interaction between the individual and the business); N.Y. Gen. Bus. Law § 899-bb(2) (requiring businesses to apply and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information, including its disposal). In addition, the Federal Trade Commission (FTC) has considered the retention of consumer data longer than a legitimate business purpose justified to be an unfair or deceptive practice under the FTC Act. (See Federal Trade Commission Act, 15 U.S.C. § 45(a) (prohibiting "unfair or deceptive acts or practices in or affecting commerce"). For more information about data minimization requirements under state laws and the FTC's interpretation of the FTC Act, see Article, Data Minimization and Avoiding the Over-Retention of Personal Information.

Maximum retention periods also commonly arise outside the US, especially in Europe. For example, the General Data Protection Regulation (GDPR) sets out a general policy that companies should retain personal data only if required for the legitimate purpose for which it was gathered. If a maximum retention period is not specifically defined by law or regulation, a record should be retained for the minimum time period established by the company as set out in the records retention schedule and then destroyed within a reasonable time after that period expires. For more information on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation.

Regardless of the expiration of the applicable retention periods, a company must keep records and information subject to a legal hold until the hold is lifted and is no longer applicable to the records or information at issue.

Legal Holds

If a company is involved in or reasonably anticipates becoming involved in litigation (including arbitration), a government investigation, or an audit, it must ensure that relevant records and information are neither deleted nor destroyed. Accordingly, companies should develop a legal hold policy that suspends normal destruction practices for records and information related to the litigation, investigation, or audit. A company also may use a legal hold or similar procedures in other exceptional circumstances requiring the retention of information beyond its ordinary period, such as a merger, divestiture, or acquisition, or following a settlement, sanction, or judgment.

Typically, employees within a company's legal department are responsible for deciding when to implement a legal hold and making other related decisions required while the legal hold is in place. In companies without a legal department, the chief operations officer or head of the information technology (IT) group should make these decisions, with the assistance of outside counsel when needed. A company usually implements a legal hold by issuing a legal hold notice (also known as a legal hold notice or document preservation notice) to those employees, officers, and directors who may have relevant records or information. If available, a company also may enable technological features that automatically preserve information.

For a sample legal hold notice, see Standard Document, Litigation Hold Notice.

When drafting a DRP, counsel should explain that a legal hold is an action undertaken by the company to preserve records and information related to an existing or a reasonably anticipated lawsuit, government investigation, or audit that:

- Suspends the ordinary destruction and disposal of records and disposable information that are subject to the legal hold.
- Overrides the retention periods set out in the records retention schedule for records that are subject to the legal hold.

By clearly explaining legal holds in the DRP, and by plainly describing in each legal hold notice the types of records and information that employees must retain or preserve, counsel can help to ensure employees do not accidentally destroy records and information that the company has a legal duty to retain or preserve.

Should the company need to defend its preservation actions, such clear definitions and descriptions may bolster the company's position on the reasonableness of its preservation efforts. When a company loses information that it should have preserved, a court will likely factor the presence and effectiveness of a legal hold into its analysis on whether to issue spoliation sanctions (FRCP 37(e); see, for example, *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 162 (2d Cir. 2012) (noting that the adoption of appropriate preservation practices is one factor in the analysis of whether to issue sanctions)).

Additionally, counsel should consider whether to include in the DRP:

- A legal hold policy. If the legal hold policy is not integrated into the DRP, the DRP should refer to it and make clear to employees that implementing a legal hold suspends retention procedures related to the affected records and information.
- A description of the steps counsel and employees must take to carry out the legal hold so that records and information subject to the hold are not discarded while the hold remains in place, or a note that these types of instructions are provided with the company's legal hold notice(s).
- Specific information about legal hold implementation, given that the DRP generally is not protected by the attorney-client privilege (for more information on the attorney-client privilege, see Attorney-Client Privilege and Work Product Doctrine Toolkit).
- Guidance regarding the restoration of retention procedures after a hold has been released.

For a collection of resources to help counsel preserve documents and implement a legal hold, see Preserving

Documents and Electronically Stored Information Toolkit and Litigation Hold Toolkit.

Identify Records and Information Subject to Retention Requirements

Designing an effective DRP involves identifying the types of information that the company should retain, typically by listing these types of records in a records retention schedule (see Records Retention Schedules). To assess the types of records a company may need to retain and for how long, counsel should consider two broad categories of information, namely information that the company:

- Should retain for internal business reasons because the information has a long-term business value for the company (see Information Retained for Internal Business Reasons).
- Must retain for legal or other external reasons (see Information Retained for Legal or Other External Reasons).

Records and Information Retained for Internal Business Reasons

Certain information holds long-term intrinsic operational or strategic value to the company, such as information that:

- Memorializes decisions and activities.
- Informs future decisions and activities.
- Allows the company to secure or defend its rights.

A company should retain this information while it has value to the business and that value outweighs the costs and risks of retaining the information. The assessment of whether and how long to retain information should reflect the perspective of multiple business stakeholders, including the business users of the information and the business functions that incur the cost of storing and managing the information (including costs associated with infrastructure, litigation and discovery, and disposition of the information).

Records and Information Retained for Legal or Other External Reasons

Certain information, regardless of its internal business value, may be subject to retention requirements arising from:

- Federal and state laws and regulations.
- Contracts.
- Sanctions.
- Other external requirements that affect how long the company must or should retain the information.

External requirements may be:

- **Set out explicitly.** These include requirements imposed by regulation or contract. For example:
  - the Occupational Safety and Health Administration (OSHA) requires most employers with 11 or more employees to retain logs of work-related injuries and illnesses for at least five years (29 C.F.R. §§ 1904.1, 1904.29, 1904.33) (for more information, see Practice Note, OSHA Injury and Illness Recordkeeping); and
  - the Employee Benefits Security Administration requires the person or entity responsible for administering a company-sponsored employee benefit plan subject to the Employee Retirement Income Security Act of 1974 (ERISA) to retain any records that must be disclosed under ERISA for at least six years from the date on which they were required to be disclosed (29 U.S.C. § 1027).
- **In the form of guidance.** Examples include regulatory agency opinion letters, position statements, and auditor procedures.

As discussed above, companies also must preserve records and information that are relevant to an ongoing or a reasonably anticipated lawsuit, government investigation, or audit involving the company (see Legal Holds). Companies issue legal hold notices to identify records and information employees must preserve under a legal hold instead of including the relevant categories of records and information in a records retention schedule.

Applications That Should Not Be Used To Create Records

A DRP should address applications that employees should not use to create records and what to do if records are created in such applications. For example, a DRP may state that employees should not create records in instant messaging applications, mobile messaging applications, or similar communication platforms and instruct employees who receive a message that constitutes a record in these applications or platforms to document the communication in an appropriate medium and retain it as a record in an appropriate repository.

Define Employee DRP Roles and Responsibilities

A DRP should outline employee responsibilities arising from the DRP and define the roles and groups within

the company that are responsible for implementing and managing the DRP. The DRP may include or link to appendices that assist employees with meeting their obligations under the DRP, such as:

- Key contact information.
- Records retention schedules.
- Records storage procedures.
- Procedures for the disposition and destruction of inactive records.
- Procedures for handling the records of separated employees.

The DRP should address the roles and responsibilities of:

- All company employees generally (see All Employees).
- Records coordinators within each business unit or department (see Records Coordinators).
- The records and information management committee tasked with supervising DRP administration (see Records and Information Management Committee).
- Other key employees, depending on the company (see Other Employees).

All Employees

Employees create, receive, and use company information in their daily business and are primarily responsible for managing that information. The DRP should clearly indicate that every employee must:

- Properly maintain and dispose of records and information consistent with the company's DRP and records retention schedules.
- Comply with other records management procedures, such as storage or naming conventions.

Supervisors should ensure that employees and third parties who create or use the company's records or information comply with the company's DRP and records retention schedules.

Records Coordinators

Typically, records coordinators (also known as records managers) are individuals within a company designated by a departmental head to:

- Oversee retention and disposal of records and information within a particular business unit or region.
- Assist their business unit or region's employees in complying with the DRP.

Records coordinators often function as the company's first line of defense in ensuring DRP compliance. They must have specific knowledge of the relevant records and information issues and the particular retention requirements for their business unit or region. Because records coordinators are embedded within particular business units or departments, they are often the first to identify specific records and information management challenges. Also, they are usually best positioned to answer questions from colleagues quickly and anticipate DRP issues before problems arise.

Records and Information Management Committee

A records and information management committee is a designated group tasked with:

- Supervising the administration of the DRP.
- Making decisions on adopting and modifying records retention schedules.
- Regularly reviewing and revising the DRP and records retention schedules as needed to keep them current.
- Strengthening the company's information management program.
- Responding to questions about how to implement the company's information management program.

Typically, the records and information management committee is made up of employees from the compliance, legal, information security, and IT departments. This ensures that all DRP stakeholders are involved when DRP decisions are made. The records and information management committee should also include senior-level employees, enabling the committee to make most DRP-related decisions without requiring additional layers of approval.

Other Employees

In addition to the individuals and roles described above, the DRP may need to address the roles of:

- **The corporate records manager.** Some companies employ a corporate records manager or officer who handles the day-to-day DRP operations and works with the records coordinators, the business units or departments, and the records and information management committee. The corporate records manager, however, needs the active involvement and cooperation of other employees to properly manage the company's records and other information.

- **Individuals responsible for making decisions related to a legal hold.** As discussed above, this responsibility may rest with the company's legal department employees, chief operations officer, or head of the IT group (see Legal Holds).

Separated Employees

A DRP should address a process to identify and retain records subject to the records retention schedule in the possession or control of separated or departed employees, which is ideally set in motion prior to the employee's departure. The DRP should also identify how the company will preserve records and information in the employee's possession or control that are subject to a legal hold. Some companies may also establish criteria for the preservation of former employees' records and information where the circumstances of the employee's departure suggest an increased risk of litigation.

Information Management Frameworks

Counsel should consider consulting standard information management frameworks when developing a DRP. The Sedona Conference and ARMA International are the two leading authorities on information management. The resources they provide emphasize that companies must develop their own DRPs and information management programs customized to their:

- Industry.
- Legal profile.
- Geographies.
- Workforce.
- Culture.
- Technology infrastructure.
- Information flows.

The Sedona Guidelines

Though it has been nearly two decades since its publication, the 2007 edition of The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (2d ed.) (Sedona Guidelines) still provides helpful tips that counsel should consider when developing a DRP. In particular, counsel should make sure the company:

- Adopts reasonable policies and procedures (see Adopt Reasonable Policies and Procedures).
- Develops a DRP that is realistic, practical, and customized to the company (see Make the DRP Realistic, Practical, and Customized).
- Incorporates procedures to avoid the unnecessary retention of all electronic information (see Do Not Unnecessarily Retain All Electronic Information).
- Takes a comprehensive approach to the information lifecycle (see Take a Comprehensive Approach).
- Mandates the suspension of ordinary destruction practices and procedures to comply with any legal holds (see Provide for a Legal Hold).

This guidance is at the heart of The Sedona Conference's more recent *Commentary on Defensible Disposition* (20 Sedona Conf. J. 179 (2019)), which encourages companies to:

- Dispose of information that it need not preserve or retain for legal reasons and that no longer has business value.
- Identify and manage the risks of over-retention.
- Base disposition on policies that reflect and integrate with their information, technological capabilities, and objectives.

Adopt Reasonable Policies and Procedures

A company's information management policies and procedures should:

- Make sense in relation to the company's circumstances.
- Be easy to understand.
- Avoid unthinkingly mandating the retention of all information and documents.

Make the DRP Realistic, Practical, and Customized

Because no model policy can fully meet all of a company's unique operational, regulatory, and IT needs, there is no single template that accommodates every company's circumstances. Counsel should:

- Evaluate operational, strategic, and legal issues to understand the value of information for retention.
- Ensure the DRP is sufficiently flexible and scalable to meet the needs of the company's various layers and groups.
- Distinguish retention requirements under the DRP from retention requirements under the company's business continuation or disaster recovery plan.

Do Not Unnecessarily Retain All Electronic Information

A company may systematically destroy information that it need not retain for business or legal reasons. In general, unless special circumstances exist, a company may:

- Adopt programs that regularly delete emails, instant messages, text messages, chats and group messages, and voicemails.
- Systematically delete backup data.
- Systematically delete residual or shadowed data.
- Set standards for the metadata the company generates in the ordinary course of business and whether the company must retain it.

Take a Comprehensive Approach

An effective DRP should consider the various issues that arise throughout the information lifecycle, which involves the creation, identification, retention, retrieval, and destruction of information. Counsel should take steps to:

- Implement the necessary retention policies and schedules.
- Document information management practices, including those that may not be included in the DRP.
- Define DRP roles and responsibilities for program direction and administration.
- Guide employees on how to identify and retain information that has a business purpose or that the company must maintain by law or regulation.
- Define the roles and responsibilities of content and technology custodians for electronic records management.
- Address the impact of existing and new technologies (including the potential benefits and risks) on the creation, retention, and destruction of records, such as the use of:
  - collaboration platforms;
  - company-owned mobile devices;
  - personal mobile devices used for work; and
  - third-party services, infrastructures, or platforms.
- Educate employees about the specific terms and provisions in the DRP. For a sample presentation to employees on records retention, see Standard Document, Document Retention: Presentation Materials.
- Conduct periodic compliance reviews of DRP procedures and respond to the findings of those reviews as appropriate.
- Coordinate the DRP with other policies concerning the use of company property and information, including applicable privacy rights or obligations.
- Implement a continuous evaluation process to update policies and practices, as needed, in response to changes in:
  - workforce;
  - company structure;
  - business practices;
  - legal or regulatory requirements; or
  - technology.

Provide for a Legal Hold

The Sedona Guidelines explain that a DRP may include instructions on how the company suspends ordinary destruction practices when necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigations, or audits. As discussed above, DRPs often include these types of instructions or reference a separate legal hold policy containing them (see Legal Holds).

Developing these instructions requires counsel to:

- Anticipate circumstances that require a legal hold and have a plan in place to implement a hold that is tailored to the company.
- Address how to effectively communicate notice of a legal hold, provide necessary training, and document the steps taken to implement the hold.
- Identify employees with the authority to suspend normal destruction procedures and impose a legal hold.

Counsel should note that it is also important for the legal hold process to include procedures for returning the suspended content to the DRP's normal information management procedures after the hold has expired.

See Standard Document, Litigation Hold Lift Notice for a sample legal hold lift notice (also known as a "legal hold release notice") to alert recipients that a legal hold is no longer in effect.

ARMA International's Generally Accepted Recordkeeping Principles®

ARMA International's Generally Accepted Recordkeeping Principles (the Principles) are another helpful guide to understanding the issues counsel should consider when

developing a DRP. The Principles can be summarized as follows:

- **Principle of accountability.** A company should assign a senior executive to:
  - oversee the recordkeeping program;
  - delegate responsibility for the recordkeeping program to appropriate individuals;
  - adopt policies and procedures to guide employees; and
  - ensure the recordkeeping program's auditability.
- **Principle of integrity.** A company should devise the recordkeeping program so that the records and information the company generates, receives, and manages have a reasonable guarantee of authenticity and reliability.
- **Principle of protection.** A company should design the recordkeeping program to ensure a reasonable level of protection to records and information that are:
  - private;
  - confidential;
  - privileged;
  - secret; or
  - essential to business continuity.
- **Principle of compliance.** The recordkeeping program should comply with:
  - applicable laws and other binding authorities; and
  - company policies.
- **Principle of availability.** The company should maintain its records and information in a way that ensures the timely, efficient, and accurate retrieval of needed information.
- **Principle of retention.** The company should maintain its records and information for an appropriate time, considering legal, regulatory, fiscal, operational, and historical requirements.
- **Principle of disposition.** The company should securely and appropriately dispose of records and information it no longer needs to maintain.
- **Principle of transparency.** The company should document its recordkeeping processes and activities in a way that all employees and appropriate parties can understand them.

ARMA International's website also provides information and links to resources regarding the international records management standard, ISO Standard 15489-1:2016, which sets out high-level guidance and best practices on designing information management programs, which companies may find useful when creating DRPs (see, for example, Nancy Dupre Barnes, ISO 15489 — Revised and Redesigned for 2016, Information Management, Sept./Oct. 2016, at 30).

Practical Considerations

An effective records management program recognizes that a company's DRP is not a stand-alone document. Instead, the DRP incorporates other policies related to records and information retention, such as policies on:

- Computer use (for more information, see Standard Document, IT Resources and Communications Systems Policy).
- Personal device use (for more information, see Standard Document, Bring Your Own Device to Work (BYOD) Policy).
- Information security (for more information, see Standard Document, Information Security Policy).
- Social media use (for more information, see Standard Documents, Social Media Policy (US) and Company Social Media Use Guidelines).
- Data privacy (for more information, see Privacy Compliance and Policies Toolkit).

Additionally, companies developing a DRP should:

- Proactively make sure that employees comply with the DRP (see Compliance).
- Instruct employees on how to integrate the DRP's processes and requirements into their daily tasks (see Records Management Documentation and Education).
- Update the DRP regularly (see Updates to the DRP).

Compliance

Companies must mandate employee compliance with the DRP. A company should explain to employees that a comprehensive and mandatory records and information management program exists and take steps to measure compliance. Clearly communicating the need for all employees to strictly comply with the DRP requires strong language, such as the following:

All company employees must comply with this policy, the records retention schedules, and any legal hold communications. Failure to do so may subject the

company, its employees, and contract staff to serious civil and/or criminal liability. Failure to comply with this policy may result in disciplinary sanctions, including dismissal or contract termination.

However, the company should not commit to stern warnings in writing unless it is willing and prepared to undertake compliance and enforcement actions.

Additionally, a company may implement an audit program, which allows the company to measure and demonstrate employee compliance with the DRP. Audits can take many forms, such as focusing on employee awareness or reviewing actual practice. Audits should assess both retention and disposal of records and information, as well as compliance with legal holds.

Records Management Documentation and Education

To effectively and consistently apply a DRP throughout a company, the company should provide employees with:

- An easily accessible resource that documents the DRP procedures (see Documentation).
- Regular training and education on how to implement the DRP procedures, especially when the DRP is updated or revised (see Education and Training Materials).

Ideally, the company maintains the DRP, records retention schedule, program documentation, and education and training materials as separate documents. This helps ensure that the DRP remains mostly static, while regular updates to other records management documentation are applied as the company changes its internal systems and processes.

Documentation

Typically, documentation of a records and information management program describes how to implement the DRP and related procedures in the company's particular information and business environment. For example, the program documentation may instruct employees on:

- How to use the company's document management system or software.
- Proper procedures for sending paper records to offsite storage, including appropriate labeling and indexing.
- Proper methods for disposing information that no longer serves a useful purpose or records that have reached the end of their retention period.
- Whom employees should contact when questions about the DRP arise.

Education and Training Materials

Records and information management education and training materials instruct employees on how to comply with the requirements of a company's DRP. These materials may be part of a company's human resources, IT, security, or business ethics policies. A company should present these materials in connection with its:

- Orientation procedures for new employees.
- Learning curriculum in a company university, where virtual or in-person class attendance is required and tracked.

Training materials should include instructions on how to comply with a legal hold notice, as well as how to properly destroy records that have met their required retention period. For example, the training manual may state that employees must shred all hard copies of financial and employee-related records when the company no longer must retain them under either the company's records retention schedule or preserve them under a legal hold.

Updates to the DRP

To maintain the accuracy of a company's DRP, counsel should:

- Review the DRP at least once each year.
- Republish updated versions of the DRP as needed.
- Distribute the updated DRP company-wide, highlighting the changes and how they affect employees' daily tasks.

The authors wish to thank those who have made significant contributions to previous versions of this Practice Note.